SIERRA COLLEGE

Job Description

JOB TITLE: Deputy Director – ITS Security and Cloud Architecture

PAY GRADE: Classified Supervisory (CS)21

LAST REVISED: June 2022

Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are not intended to reflect all duties performed within the job. Additional or different duties from the ones set forth below may be required to address changing business needs/practices.

Under the direction of the Chief Technology Officer, the Deputy Director, ITS Security and Cloud Architecture performs a variety of responsible and complex duties, designing and implementing a comprehensive information security program which includes strategies, standards, policies, procedures, and response plans designed to protect the confidentiality, integrity, and availability of enterprise systems and data throughout the district, and also overseeing the design and implementation of the district's enterprise cloud environment.

Sierra College has a strong commitment to the achievement of equity and inclusion among its faculty, staff and students and values the rich diverse backgrounds that make up the campus community. The Deputy Director-ITS Security and Cloud Architecture must demonstrate a profound understanding of and experience with successfully supporting individuals with varying backgrounds. This includes persons with disabilities, various gender identities, sexual orientation, individuals from historically underrepresented communities and other groups to ensure the District provides strategies for success and pro-active, student-centered practices and policies committed to eliminating equity gaps.

REPRESENTATIVE DUTIES - *The following duties are typical for this classification. Incumbents may not perform all of the listed duties and/or may be required to perform additional or different duties from those set forth below to address business needs and changing business practices.*

1. Provides overall vision and leadership for the district in all areas of information security, acting as a technical liaison with college technology governance committees, working groups, and district staff in facilitating development of a comprehensive information security program.
2. Develops, recommends, implements, and maintains information security policies, procedures, protocols, and standards pertaining to managing the protection and security risk of college data and IT systems and assets.
3. Oversees and participates in risk analysis of IT infrastructure and systems to isolate potential threats and hazards; assesses the potential impact on business assets; develops a risk management strategy that uses the district's priorities, constraints, and risk tolerances to support operational risk decisions.
4. Implements processes and systems to identify and manage district assets consistent with their relative importance to organizational objectives and the organization's risk strategy.
5. Helps oversee Data Governance frameworks, policies, and procedures; develops, implements, and enforces Data Classification rules and procedures; develops systems and processes for tracking locations and securing confidential data, including Personally Identifiable Information (PII).
6. Oversees management of user identity and access control, including limiting of access to information assets based on Data Classification policies and procedures, auditing the use of privileged accounts, and use of Multi-Factor Authentication.

7. Conducts assessments and audits to evaluate whether security compliance requirements are met for federal, state, and local legislation related to information security, including but not limited to, FERPA, GLBA, HIPAA, GDPR, and CCPA; help facilitate compliance with section 508 accessibility laws.
8. Creates and maintains a security awareness training program to increase security vigilance and knowledge of employees, students, and vendors to help minimize information security risks.
9. Implements and maintains security monitoring systems to send out alarms and alerts for IT security issues for all technology assets; use those systems to identify, diagnose, resolve, and report IT security problems and incidents; coordinate and conduct investigations of breaches in IT Security; respond to emergency IT security situations.
10. Develops and maintains security Incident Response Plans for the district's critical systems; assures plans are periodically tested and updated, utilizing metrics and evaluation criteria to assess effectiveness and continually improve response performance; engages, interacts, and coordinates with third-party incident responders, including cyber-insurance providers and law enforcement; incorporates lessons learned to improve plans.
11. Designs, implements, maintains, and tests disaster recovery and business continuity plans for critical district systems; oversees scheduled testing of plans.
12. Consistent with policies and procedures, ensures that maintenance, configuration, repair, and patching of systems occurs on a scheduled and timely basis utilizing best practices in change management.
13. Manages relationships with vendors that provide security-related services, including monitoring, auditing, remediation, and penetration testing; directs the work of contractors and vendors as warranted.
14. Vets and reviews security practices and controls of third-party service providers that handle college confidential data, including personally identifiable information of students and employees. Review security controls and features of third-party software systems.
15. Keeps current with latest emerging security issues and threats through list servers, blogs, newsletters, conferences, user groups, and networking and collaboration with peers at other institutions.
16. Develops cloud migration plans and strategies; develops district-wide cloud standards and practices
17. Manages relationships with cloud service providers.
18. Manages cloud expenditures, utilizing cloud platform and third-party tools to keep operational expenditures within budgets.
19. Where possible, works with Applications and Development team to redesign and refactor applications to be optimized to run natively in the cloud.
20. Supervises, directs, guides, motivates, trains, and evaluates information security staff engaged in implementing, configuring, and maintaining the district's security systems and processes.
21. Plans and manages the unit's operating budget and program budgets for initiatives and projects.
22. Performs other related duties as assigned.

QUALIFICATIONS

Experience and Education Guidelines - *Any combination of education and experience that would likely provide the required knowledge and abilities is qualifying. A typical way to obtain the knowledge and abilities would be:*

Experience:

Five (5) years of full-time equivalent experience working with information security, with at least two (2) years in a management capacity.

Education:

Education equivalent to a bachelor's degree (120 semester units) in Management Information Systems (MIS), Computer Science, Information Technology, Business Administration, or a computer-related field from an accredited institution,

OR
Seven (7) years or more working directly on developing and supporting information security may be substituted for the education requirements.

Desirable Qualifications:

Experience in a higher education environment.
Experience with complex applications such as ERP systems.

DEMONSTRATED KNOWLEDGE AND ABILITIES:

Position requires knowledge of:

- Advanced knowledge of the design, implementation, and maintenance of complex information security systems.
- Information security best practices and standards.
- Information security compliance standards and frameworks.
- Experience with public cloud environments.
- Emerging technologies and trends in information security and cloud infrastructure.
- Current principles, practices, and standards of planning and project management, project prioritization, and resource allocation.
- Section 504 and 508 Accessibility and related standards and requirements.
- Methods to successfully support individuals with varying backgrounds, which includes persons with disabilities, various gender identities, sexual orientation, individuals from historically underrepresented communities and other groups.

Ability to:

- Use leadership and management theories and practices in carrying out daily responsibilities.
- Engage in management and creative organizational leadership.
- Develop the leadership skills of others.
- Lead, implement, and manage change.
- Perform short-and-long-range planning to be successful in interpersonal relationships and evaluate the effectiveness of programs, personnel, and relationships.
- Supervise, develop, assign, and evaluate staff for efficient operation of the department.
- Plan, develop, manage, and administer complex departmental operation budgets and contracts demonstrating knowledge of sound fiscal management principles and practices.
- Logically and realistically evaluate systems and procedures.
- Meet deadlines and expedite procedures within area of responsibility.
- Compile clear, timely, accurate written reports.
- Communicate effectively both orally and in writing with faculty, staff, and state agencies.
- Establish and maintain effective working relationships with college faculty, staff, and representatives of local, state, and federal agencies.
- Plan, organize, and manage complex purchase processes, including negotiations with vendors for hardware and software acquisitions that maximize the utilization of available resources and enhance organizational efficiency.
- Communicate with peers, subordinates, supervisors, and students in an open, honest manner and build trust among all constituencies in the District.
- Be an effective and motivational member of a team.
- Demonstrate clear evidence of sensitivity to and understanding of the diverse academic, socioeconomic, cultural, disability and ethnic backgrounds of community college students, staff, and the community.

PHYSICAL DEMANDS AND WORKING ENVIRONMENT - *The conditions herein are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential job functions.*

Environment: Work is performed primarily in a standard office setting.

Physical: Primary functions require sufficient physical ability and mobility to work in an office setting; to stand or sit for prolonged periods of time; to occasionally walk, stoop, bend, kneel, crouch, reach, and twist; to lift, carry, push, and/or pull light to moderate amounts of weight; to operate office equipment requiring repetitive hand movement and fine coordination including use of a computer keyboard; and to verbally communicate to exchange information.

Vision: See in the normal visual range with or without correction; vision sufficient to read computer screens and printed documents; and to operate assigned equipment.

Hearing: Hear in the normal audio range with or without correction.